Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 3)
You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.
You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

A. the Azure landing zone accelerator
B. the Azure Will-Architected Framework
C. Azure Security Benchmark v3
D. Azure Advisor

Answer: A

NEW QUESTION 2
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling adaptive network hardening.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
JIT:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s
Adaptive Network Hardening:
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify

NEW QUESTION 3
- (Exam Topic 3)
Your company has the virtual machine infrastructure shown in the following table.

Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure. You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks
such as ransomware.
What should you include in the recommendation?

A. Use geo-redundant storage (GRS).
B. Use customer-managed keys (CMKs) for encryption.
C. Require PINs to disable backups.
D. Implement Azure Site Recovery replication.

Answer: C

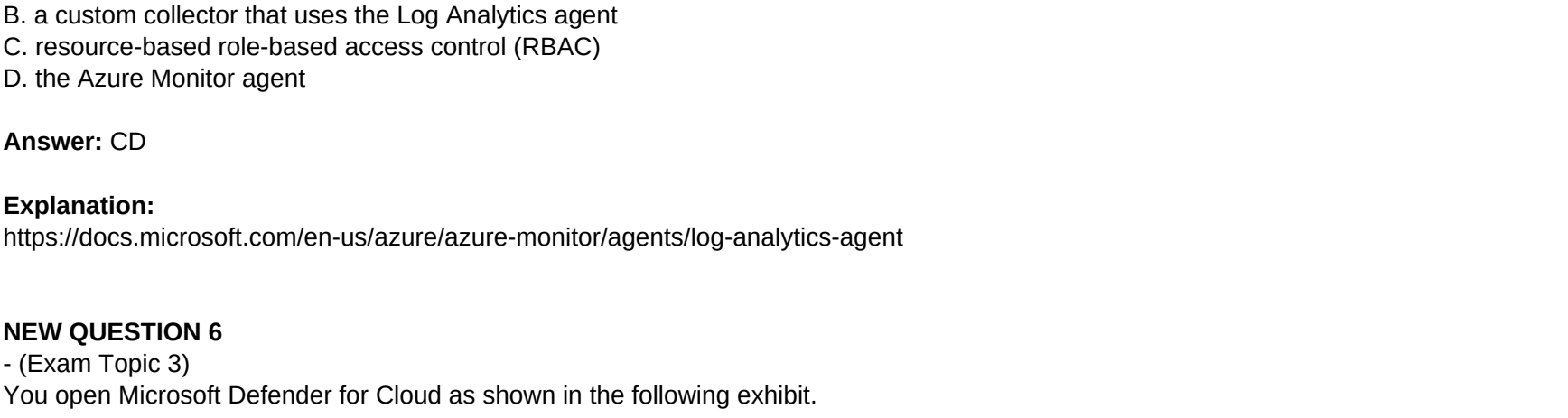
Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#azure

NEW QUESTION 4
- (Exam Topic 3)
You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. AJI the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.
You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:
• A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
• A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers
What should you use for each risk? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

A. Mastered
B. Not Mastered

Answer: A

Explanation:



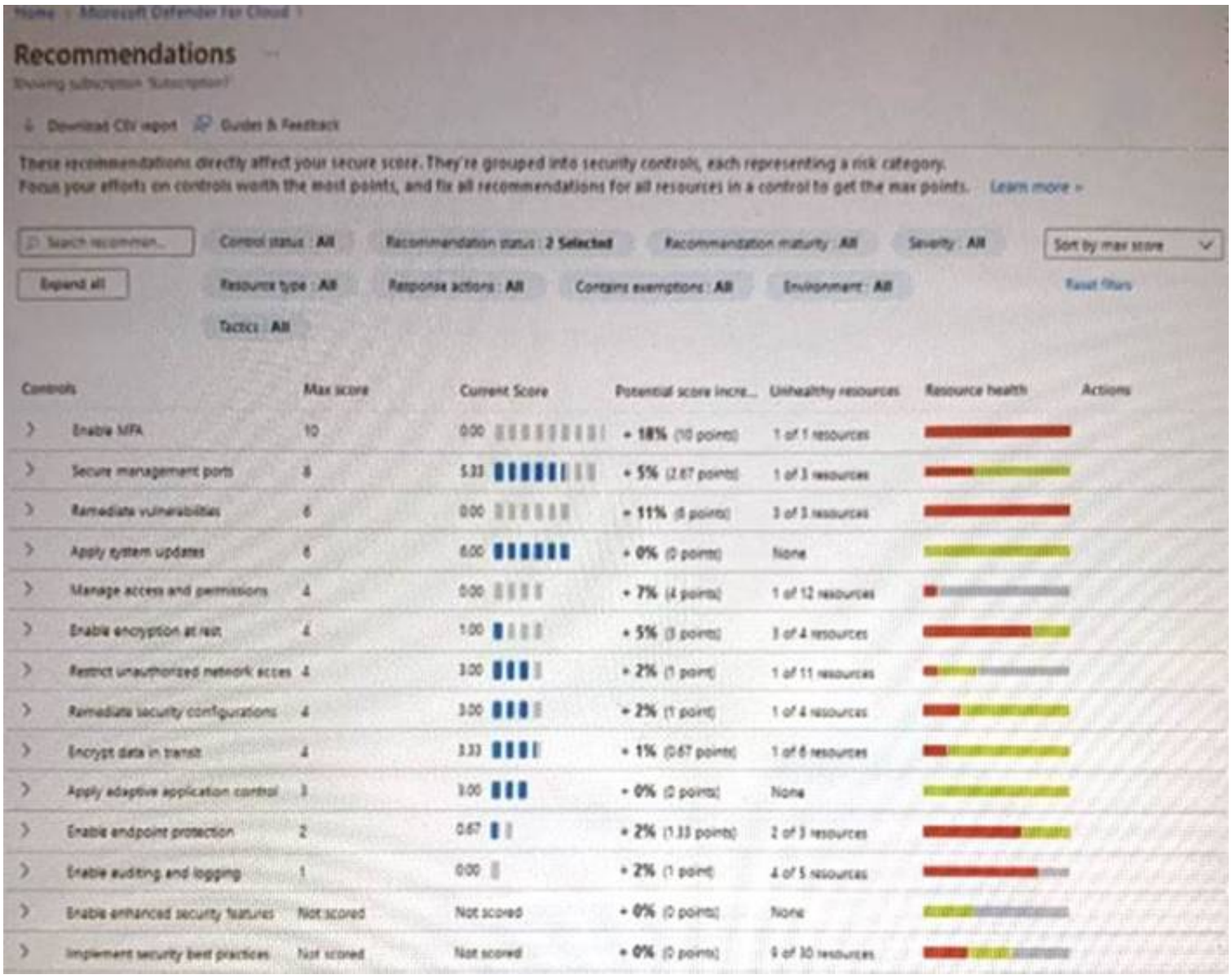
NEW QUESTION 5
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend configurations to meet the following requirements:
• Ensure that the security operations team can access the security logs and the operation logs.
• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Active Directory (Azure AD) Conditional Access policies
B. a custom collector that uses the Log Analytics agent
C. resource-based role-based access control (RBAC)
D. the Azure Monitor agent

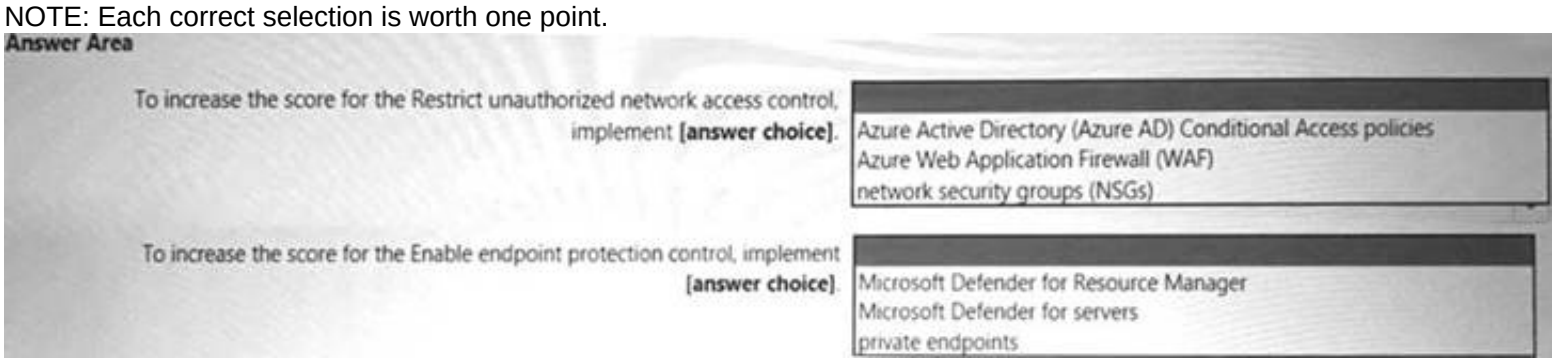
Answer: CD

Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

NEW QUESTION 6
- (Exam Topic 3)
You open Microsoft Defender for Cloud as shown in the following exhibit.



Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

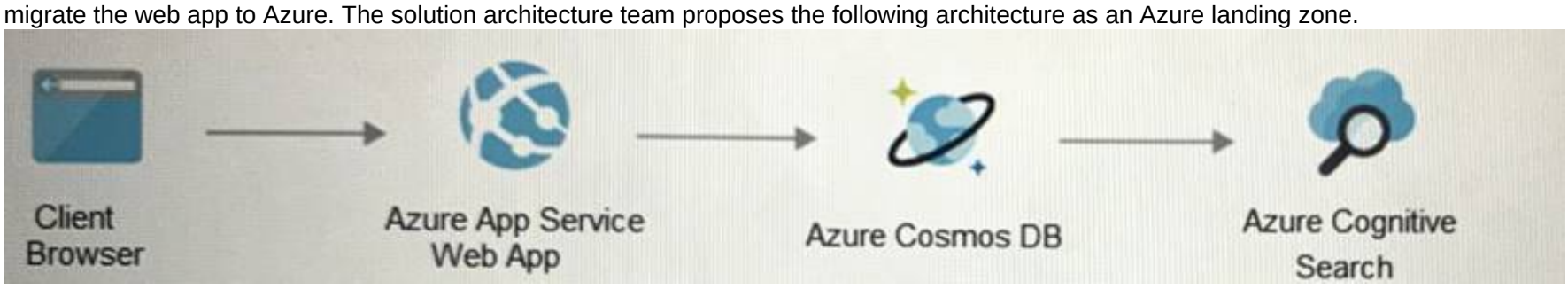


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Selection 1: NSG Selection
Selection 2: Microsoft Defender for servers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION 7
- (Exam Topic 3)
Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://www.varonis.com/blog/securing-access-azure-webapps

NEW QUESTION 8
- (Exam Topic 3)
You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers.
In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Registry
B. Linux containers deployed to Azure Kubernetes Service (AKS)
C. Windows containers deployed to Azure Container Registry
D. Windows containers deployed to Azure Kubernetes Service (AKS)
E. Linux containers deployed to Azure Container Instances

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-sec https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabi

NEW QUESTION 9
- (Exam Topic 3)
You have Microsoft Defender for Cloud assigned to Azure management groups. You have a Microsoft Sentinel deployment.
During the triage of alerts, you require additional information about the security events, including suggestions for remediation. Which two components can you use to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. workload protections in Defender for Cloud
B. threat intelligence reports in Defender for Cloud
C. Microsoft Sentinel notebooks
D. Microsoft Sentinel threat intelligence workbooks

Answer: BD

Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports https://docs.microsoft.com/en-us/azure/sentinel/notebooks

NEW QUESTION 10
- (Exam Topic 3)
You are designing a ransomware response plan that follows Microsoft Security Best Practices.
You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files. What should you include in the recommendation?

A. Microsoft Defender for Endpoint
B. Windows Defender Device Guard
C. protected folders
D. Azure Files
E. BitLocker Drive Encryption (BitLocker)

Answer: E

NEW QUESTION 10
- (Exam Topic 3)
You have a customer that has a Microsoft 365 subscription and an Azure subscription.
The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

A. Microsoft Information Protection
B. Microsoft Defender for Endpoint
C. Microsoft Sentinel
D. Microsoft Endpoint Manager

Answer: D

Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboa

NEW QUESTION 13
- (Exam Topic 3)
Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel. You plan to integrate Microsoft Sentinel with Splunk.
You need to recommend a solution to send security events from Microsoft Sentinel to Splunk. What should you include in the recommendation?

A. Azure Event Hubs
B. Azure Data Factor
C. a Microsoft Sentinel workbook
D. a Microsoft Sentinel data connector

Answer: D

Explanation:

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-ev

NEW QUESTION 16
- (Exam Topic 3)
Your company has an on-premises network and an Azure subscription.
The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.
You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.
You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.
What should you include in the recommendation?

A. a private endpoint
B. hybrid connections
C. virtual network NAT gateway integration
D. virtual network integration

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections

NEW QUESTION 19
- (Exam Topic 3)
You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Add Microsoft Sentinel data connectors.
B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Answer: A

NEW QUESTION 23
- (Exam Topic 3)
You are designing a ransomware response plan that follows Microsoft Security Best Practices
You need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out.
What should you include in the recommendations?

A. Privileged Access Workstations (PAWs)
B. emergency access accounts
C. device compliance policies
D. Customer Lockbox for Microsoft Azure

Answer: B

NEW QUESTION 24
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend configurations to meet the following requirements:
• Ensure that the security operations team can access the security logs and the operation logs.
• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
B. Use the Azure Monitor agent with the multi-homing configuration.
C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
D. Create a custom collector that uses the Log Analytics agent.

Answer: BC

NEW QUESTION 26
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription.
You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.
You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.
Which two components should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. data loss prevention (DLP) policies
B. sensitivity label policies
C. retention label policies
D. eDiscovery cases

Answer: AB

Explanation:
Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.
Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate.Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used along-side capabilities likeMicrosoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.
https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/ https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?vie

NEW QUESTION 29
- (Exam Topic 3)
You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service. You are migrating the on-premises infrastructure to a cloud-only infrastructure.
You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.
Which identity service should you include in the recommendation?

A. Azure Active Directory Domain Services (Azure AD DS)
B. Azure Active Directory (Azure AD) B2C
C. Azure Active Directory (Azure AD)
D. Active Directory Domain Services (AD DS)

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

NEW QUESTION 34
- (Exam Topic 3)
You have Windows 11 devices and Microsoft 365 E5 licenses.
You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites. What should you include in the recommendation?

A. Microsoft Endpoint Manager
B. Compliance Manager
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Endpoint

Answer: D

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-w

NEW QUESTION 35
- (Exam Topic 3)
Your company has devices that run either Windows 10, Windows 11, or Windows Server. You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune
B. Policy Analyzer
C. Local Group Policy Object (LGPO)
D. Windows Autopilot

Answer: B

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework

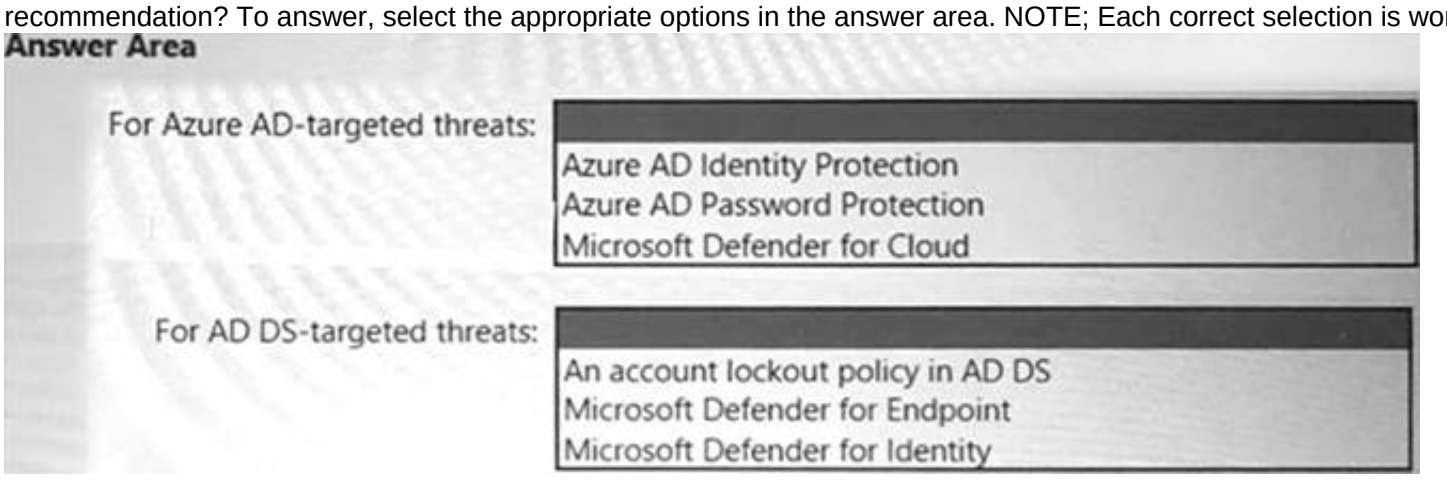
NEW QUESTION 38
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

A. insider risk management policies
B. data loss prevention (DLP) policies
C. sensitivity label policies
D. retention policies

Answer: C

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

NEW QUESTION 41
- (Exam Topic 2)
You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE; Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Azure AD Identity Protection Brute Force Detection:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
* 2. Defender for Identity
MDI can detect brute force attacks: ref:
https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts#suspected-brute-force-at

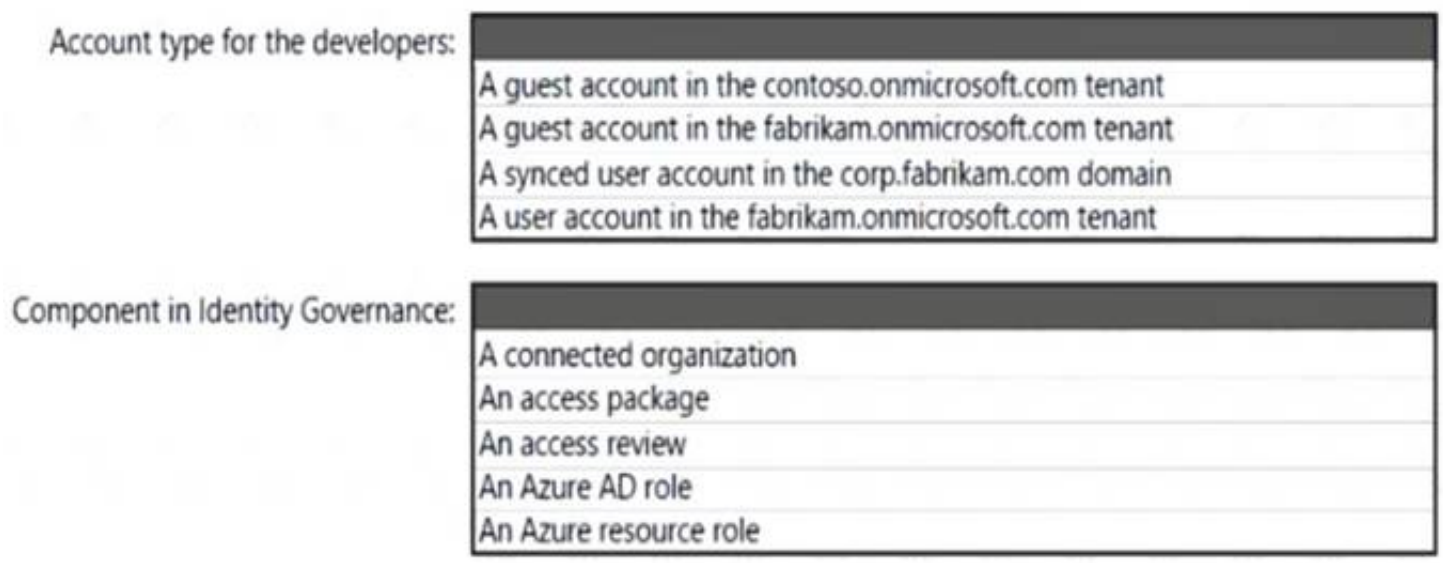
NEW QUESTION 45
- (Exam Topic 2)
You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.

A. Azure AD Conditional Access
B. Microsoft Defender for Cloud Apps
C. Microsoft Defender for Cloud
D. Microsoft Defender for Endpoint
E. access reviews in Azure AD

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#c https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cl

NEW QUESTION 49
- (Exam Topic 1)
What should you create in Azure AD to meet the Contoso developer requirements?



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: A synced user account - Need to use a synched user account.
Box 2: An access review
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/synchronization https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

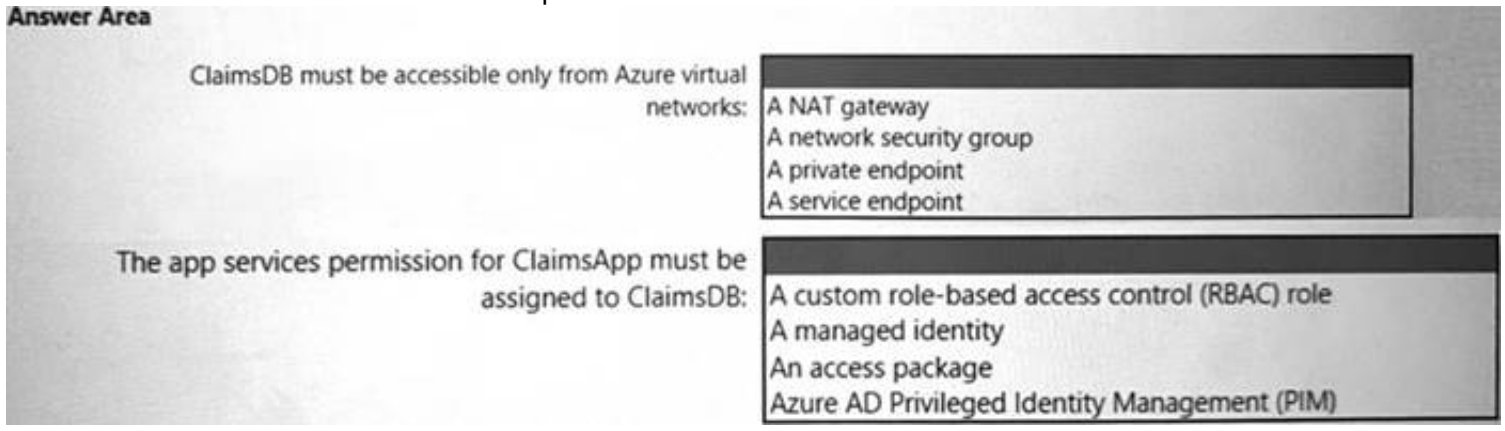
NEW QUESTION 53
- (Exam Topic 1)
You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.
What should you include in the recommendation?

A. Transparent Data Encryption (TDE)
B. Always Encrypted
C. row-level security (RLS)
D. dynamic data masking
E. data classification

Answer: D

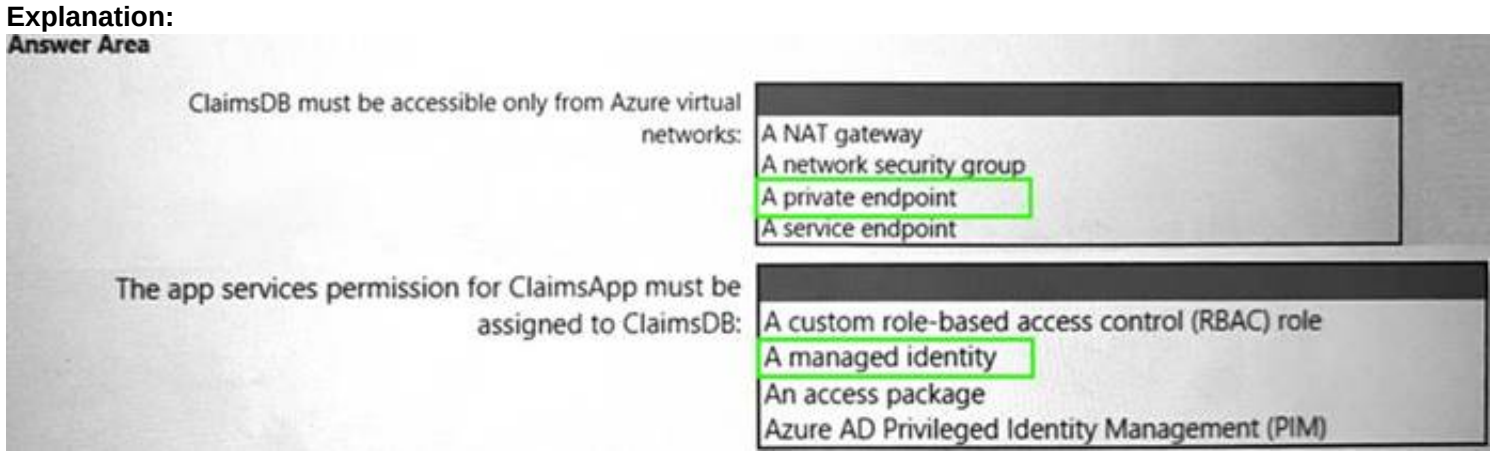
Explanation:
https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-encl

NEW QUESTION 58
- (Exam Topic 1)
You need to recommend a solution to meet the requirements for connections to ClaimsDB.
What should you recommend using for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:


NEW QUESTION 62
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend configuring gateway-required virtual network integration. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure

NEW QUESTION 67
- (Exam Topic 3)
Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access integration with user flows and custom policies
B. Azure AD workbooks to monitor risk detections
C. custom resource owner password credentials (ROPC) flows in Azure AD B2C
D. access packages in Identity Governance

E. smart account lockout in Azure AD B2C

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management
https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

NEW QUESTION 70
- (Exam Topic 3)
Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:
• Computers that run either Windows 10 or Windows 11
• Tablets and phones that run either Android or iOS
You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored. What should you include in the recommendation?

A. eDiscovery
B. retention policies
C. Compliance Manager
D. Microsoft Information Protection

Answer: D

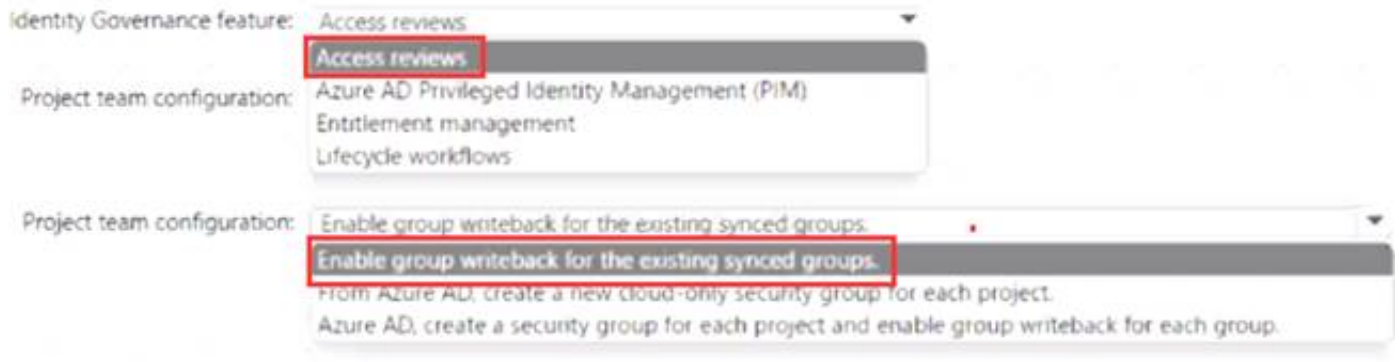
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

NEW QUESTION 72
- (Exam Topic 3)
Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders The domain syncs with Azure AD by using Azure AD Connect Azure AD Connect has group writeback enabled.
You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.
You have multiple project teams. Each team has an AD DS group that syncs with Azure AD Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.
You need to recommend an Azure AD identity Governance solution that meets the following requirements:
• Project managers must verify that their project group contains only the current members of their project team
• The members of each project team must only have access to the resources of the project to which they are assigned
• Users must be removed from a project group automatically if the project manager has MOT verified the group s membership for 30 days.
• Administrative effort must be minimized.
What should you include in the recommendation? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 75
- (Exam Topic 3)
A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.
The customer discovers that several endpoints are infected with malware. The customer suspends access attempts from the infected endpoints.
The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Endpoint reports the endpoints as compliant.
B. Microsoft Intune reports the endpoints as compliant.
C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
D. The client access tokens are refreshed.

Answer: CD

Explanation:
https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

NEW QUESTION 78
- (Exam Topic 3)
Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD). You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications. What should you include in the recommendation?

A. activity policies in Microsoft Defender for Cloud Apps
B. sign-in risk policies in Azure AD Identity Protection
C. device compliance policies in Microsoft Endpoint Manager
D. Azure AD Conditional Access policies
E. user risk policies in Azure AD Identity Protection

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-loca https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules

NEW QUESTION 82
- (Exam Topic 3)
Your company, named Contoso. Ltd... has an Azure AD tenant namedcontoso.com. Contoso has a partner company named Fabrikam. Inc. that has an Azure AD tenant named fabrikam.com. You need to ensure that helpdesk users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:
• Follow the principle of least privilege.
• Minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 86
- (Exam Topic 3)

A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.
You need to recommend a solution for the customer. The solution must minimize costs. What should you include in the recommendation?

A. Microsoft 365 Defender
B. Microsoft Defender for Cloud
C. Microsoft Defender for Cloud Apps
D. Microsoft Sentinel

Answer: D

NEW QUESTION 91
- (Exam Topic 3)
You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:
• Prevent the need to enable ports 3389 and 22 from the internet.
• Only provide permission to connect the virtual machines when required.
• Ensure that administrators use the Azure portal to connect to the virtual machines.
Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
B. Configure Azure VPN Gateway.
C. Enable Just Enough Administration (JEA).
D. Enable just-in-time (JIT) VM access.
E. Configure Azure Bastion.

Answer: DE

Explanation:
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

NEW QUESTION 92
- (Exam Topic 3)
Your company plans to provision blob storage by using an Azure Storage account The blob storage will be accessible from 20 application sewers on the internet.
You need to recommend a solution to ensure that only the application servers can access the storage account. What should you recommend using to secure the blob storage?

A. service tags in network security groups (NSGs)
B. managed rule sets in Azure Web Application Firewall (WAF) policies
C. inbound rules in network security groups (NSGs)
D. firewall rules for the storage account
E. inbound rules in Azure Firewall

Answer: D

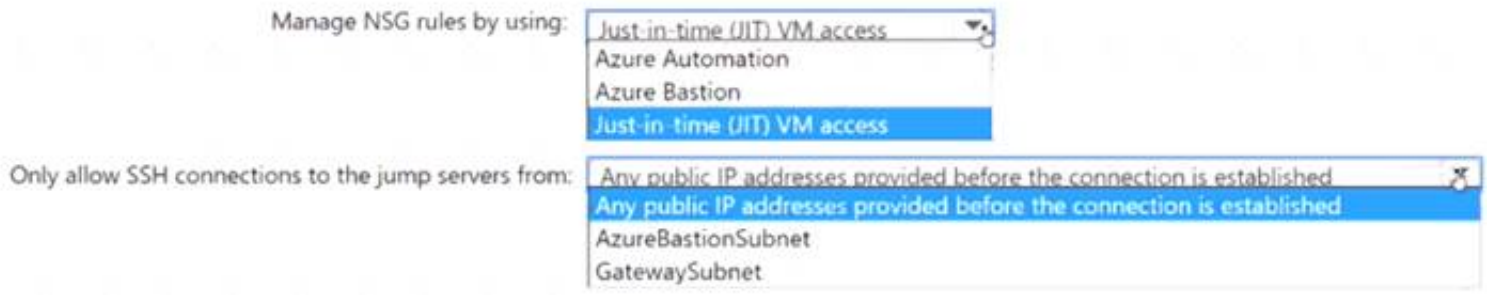
NEW QUESTION 93
- (Exam Topic 3)
Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.
You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.
You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.
What should you include in the recommendation?

A. custom roles in Azure Pipelines
B. branch policies in Azure Repos
C. Azure policies
D. custom Azure roles

Answer: B

NEW QUESTION 96
- (Exam Topic 3)
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect f personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG)
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
• Ensure that each time the support staff connects to a jump server; they must request access to the server.
• Ensure that only authorized support staff can initiate SSH connections to the jump servers.
• Maximize protection against brute-force attacks from internal networks and the internet.
• Ensure that users can only connect to the jump servers from the internet.
• Minimize administrative effort
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

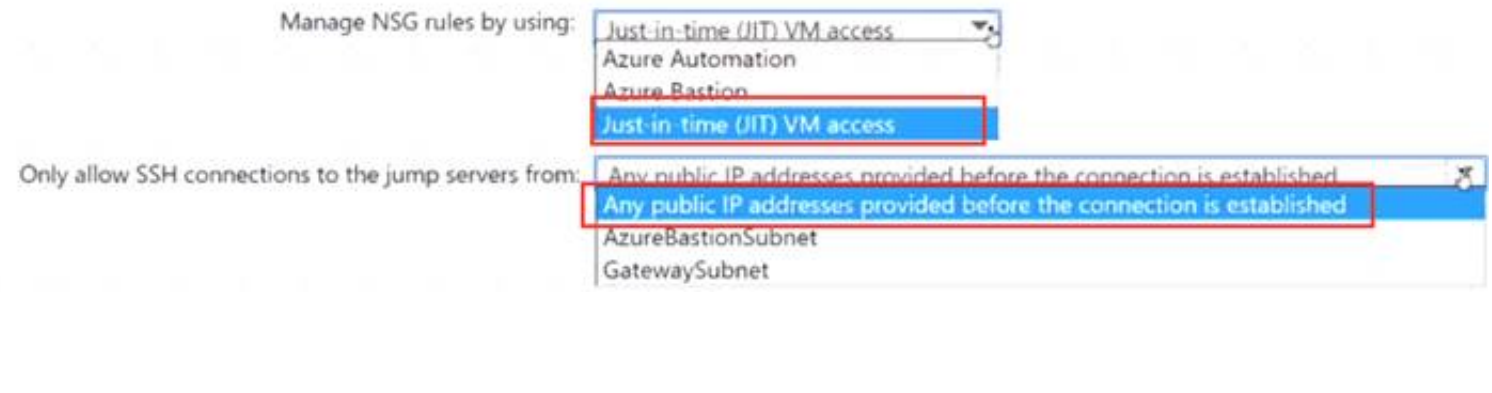
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 97
- (Exam Topic 3)
You have legacy operational technology (OT) devices and IoT devices.
You need to recommend best practices for applying Zero Trust principles to the OT and IoT devices based on the Microsoft Cybersecurity Reference Architectures (MCRA). The solution must minimize the risk of disrupting business operations.
Which two security methodologies should you include in the recommendation? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point

A. passive traffic monitoring
B. active scanning
C. threat monitoring
D. software patching

Answer: CD

NEW QUESTION 98
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.
The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.
You have remote users who have personal devices that run Windows 11.
You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:
• Prevent the remote users from accessing any other resources on the network.
• Support Azure Active Directory (Azure AD) Conditional Access.
• Simplify the end-user experience.
What should you include in the recommendation?

A. Azure AD Application Proxy
B. Azure Virtual WAN
C. Microsoft Tunnel
D. web content filtering in Microsoft Defender for Endpoint

Answer: A

Explanation:
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

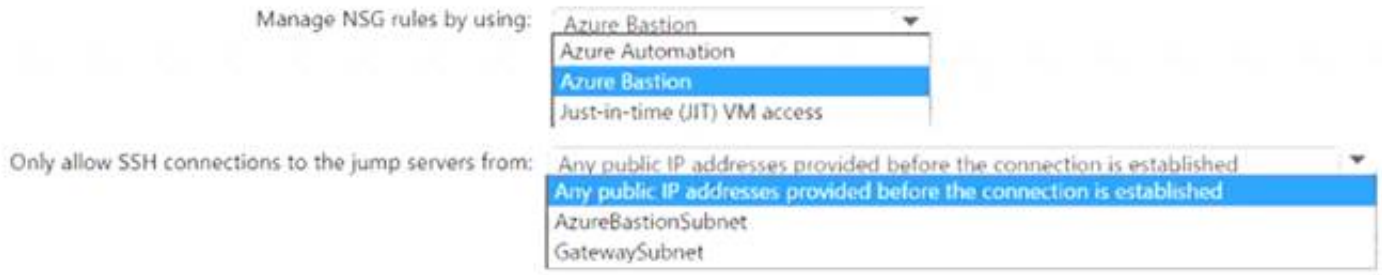
NEW QUESTION 103
- (Exam Topic 3)
You have an Azure subscription.
Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.
What should you recommend using to enforce the governance requirement?

A. regulatory compliance standards in Microsoft Defender for Cloud
B. custom Azure roles
C. Azure Policy assignments
D. Azure management groups

Answer: C

NEW QUESTION 105
- (Exam Topic 3)
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG).
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
• Ensure that each time the support staff connects to a jump server; they must request access to the server.
• Ensure that only authorized support staff can initiate SSH connections to the jump servers.
• Maximize protection against brute-force attacks from internal networks and the internet.
• Ensure that users can only connect to the jump servers from the internet.
• Minimize administrative effort.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

NEW QUESTION 110
- (Exam Topic 3)
For of an Azure deployment you are designing a security architecture based on the Microsoft Cloud Security Benchmark. You need to recommend a best practice for implementing service accounts for Azure API management What should you include in the recommendation?

A. device registrations in Azure AD
B. application registrations m Azure AD
C. Azure service principals with certificate credentials
D. Azure service principals with usernames and passwords
E. managed identities in Azure

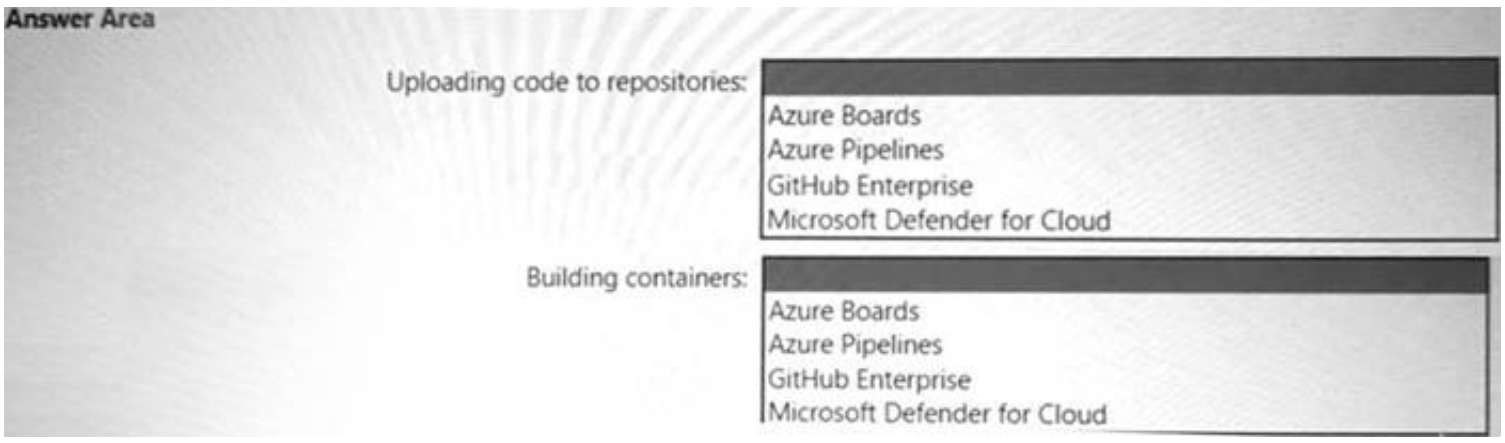
Answer: E

NEW QUESTION 114
- (Exam Topic 3)
You have an Azure AD tenant that syncs with an Active Directory Domain Services {AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.
You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.
You plan to remove all the domain accounts from the Administrators group on the Windows computers. You need to recommend a solution that will provide users with administrative access to the Windows
computers only when access is required. The solution must minimize the lateral movement of ransomware
attacks if an administrator account on a computer is compromised.
What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)
B. Privileged Access Workstations (PAWs)
C. Azure AD Privileged Identity Management (PIM)
D. Azure AD identity Protection

Answer: A

NEW QUESTION 119
- (Exam Topic 3)
Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:
Uploading the code to repositories Building containers
Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-conta

NEW QUESTION 124
- (Exam Topic 3)
Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.
The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.
Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.
You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency tor developers.
Which three actions should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
B. Implement Azure Firewall to restrict host pool outbound access.
C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
E. Deploy a Remote Desktop server to an Azure region located in France.

Answer: BCD

Explanation:
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

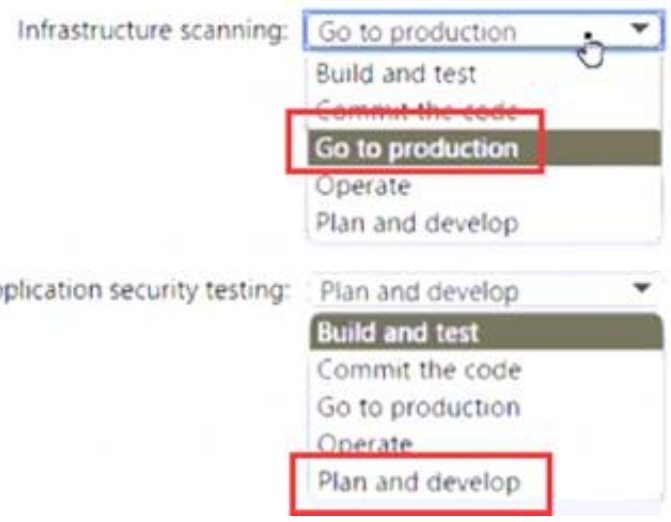
NEW QUESTION 128
- (Exam Topic 3)
Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines
You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines. What should recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

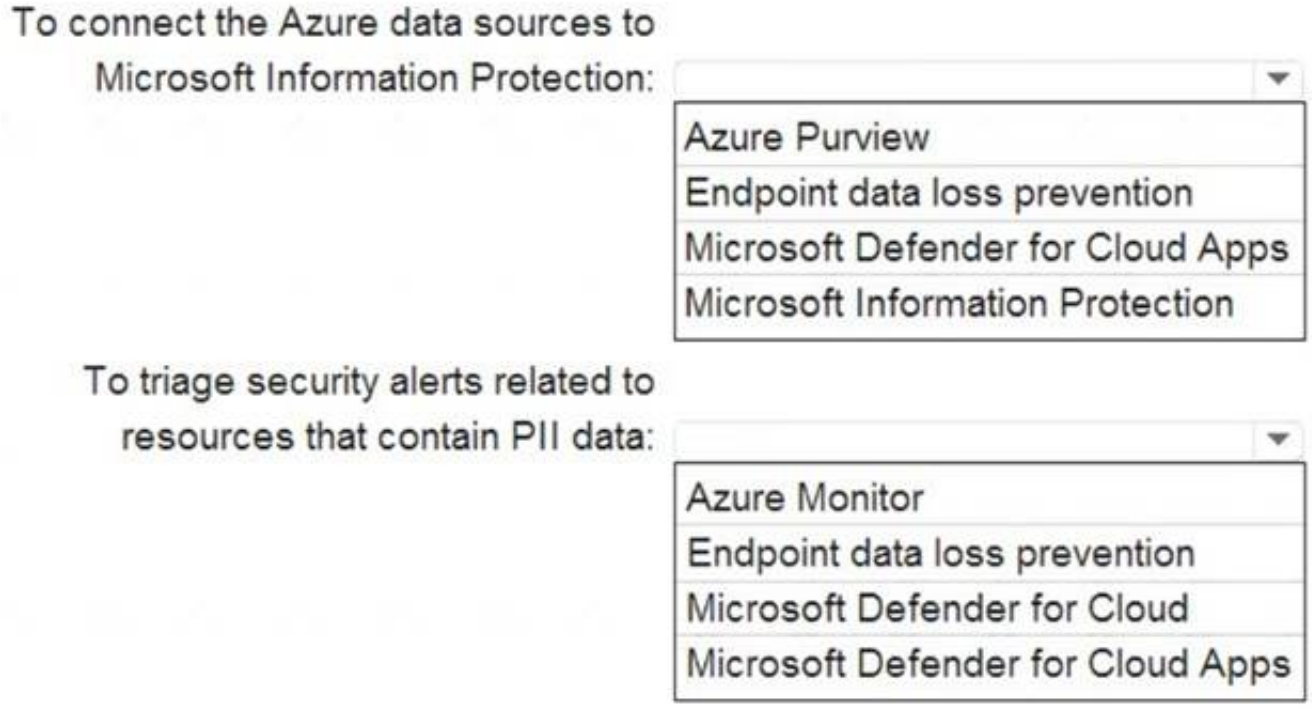
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area





NEW QUESTION 132
- (Exam Topic 3)
Your company is migrating data to Azure. The data contains Personally Identifiable Information (Pll). The
company plans to use Microsoft Information Protection for the Pll data store in Azure. You need to recommend a solution to discover Pll data at risk in the Azure resources.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Prioritize security actions by data sensitivity,
https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection. As to Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics (Azure resources as well): https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azu

NEW QUESTION 134
- (Exam Topic 3)
You have an Azure subscription that contains a Microsoft Sentinel workspace.
Your on-premises network contains firewalls that support forwarding event logs m the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls
You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel. What should you include m the recommendation?

A. an Azure logic app
B. an on-premises Syslog server
C. an on-premises data gateway
D. Azure Data Factory

Answer: B

NEW QUESTION 137
- (Exam Topic 3)
You plan to automate the development and deployment of a Nodejs-based app by using GitHub. You need to recommend a DevSecOps solution for the app. The solution must meet the following
requirements:
• Automate the generation of pull requests that remediate identified vulnerabilities.
• Automate vulnerability code scanning for public and private repositories.

• Minimize administrative effort.
• Minimize costs.
What should you recommend using? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

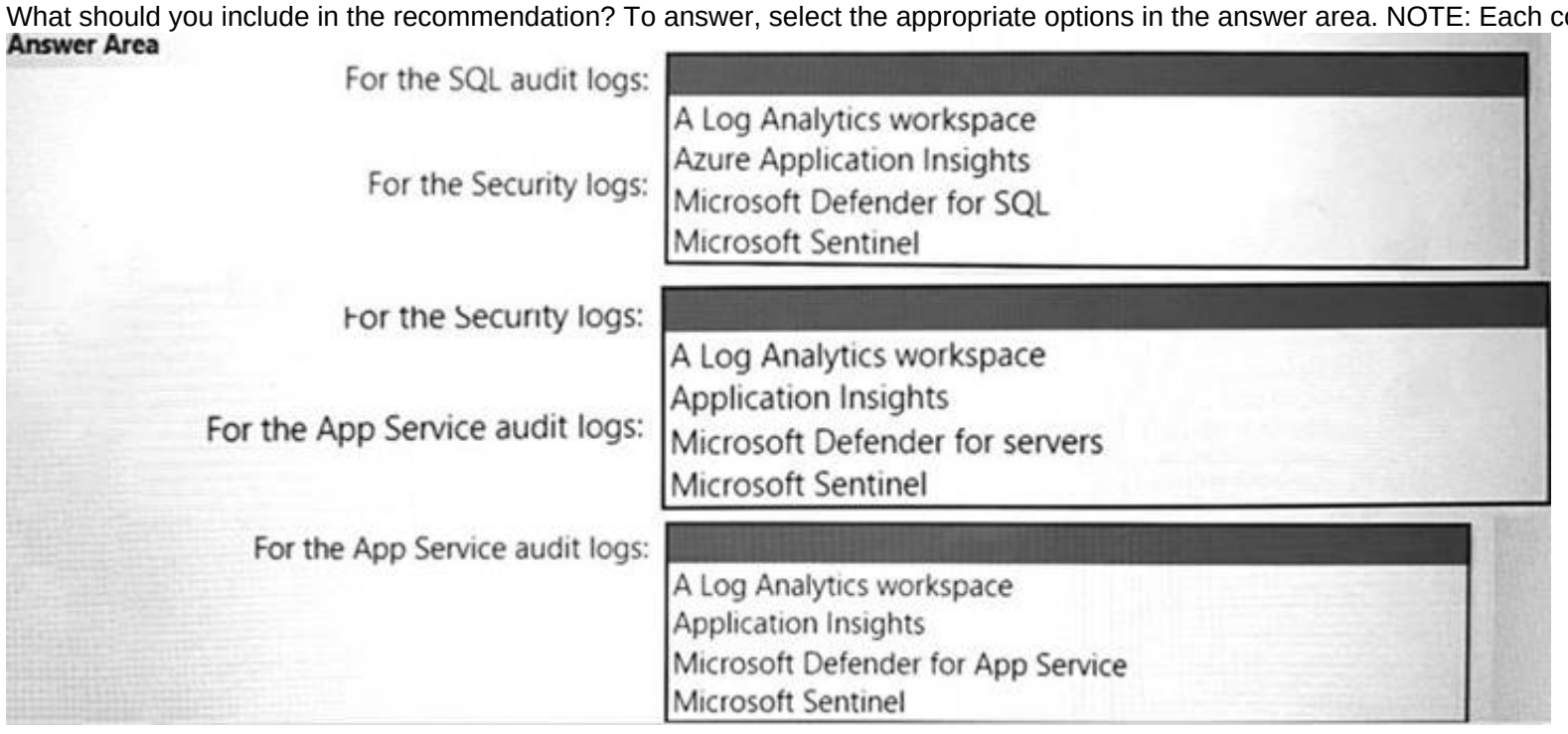
A. Mastered
B. Not Mastered

Answer: A

Explanation:
A close up of a text Description automatically generated

NEW QUESTION 141
- (Exam Topic 3)
You are designing an auditing solution for Azure landing zones that will contain the following components:
• SQL audit logs for Azure SQL databases
• Windows Security logs from Azure virtual machines
• Azure App Service audit logs from App Service web apps
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
• Log all privileged access.
• Retain logs for at least 365 days.
• Minimize costs.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

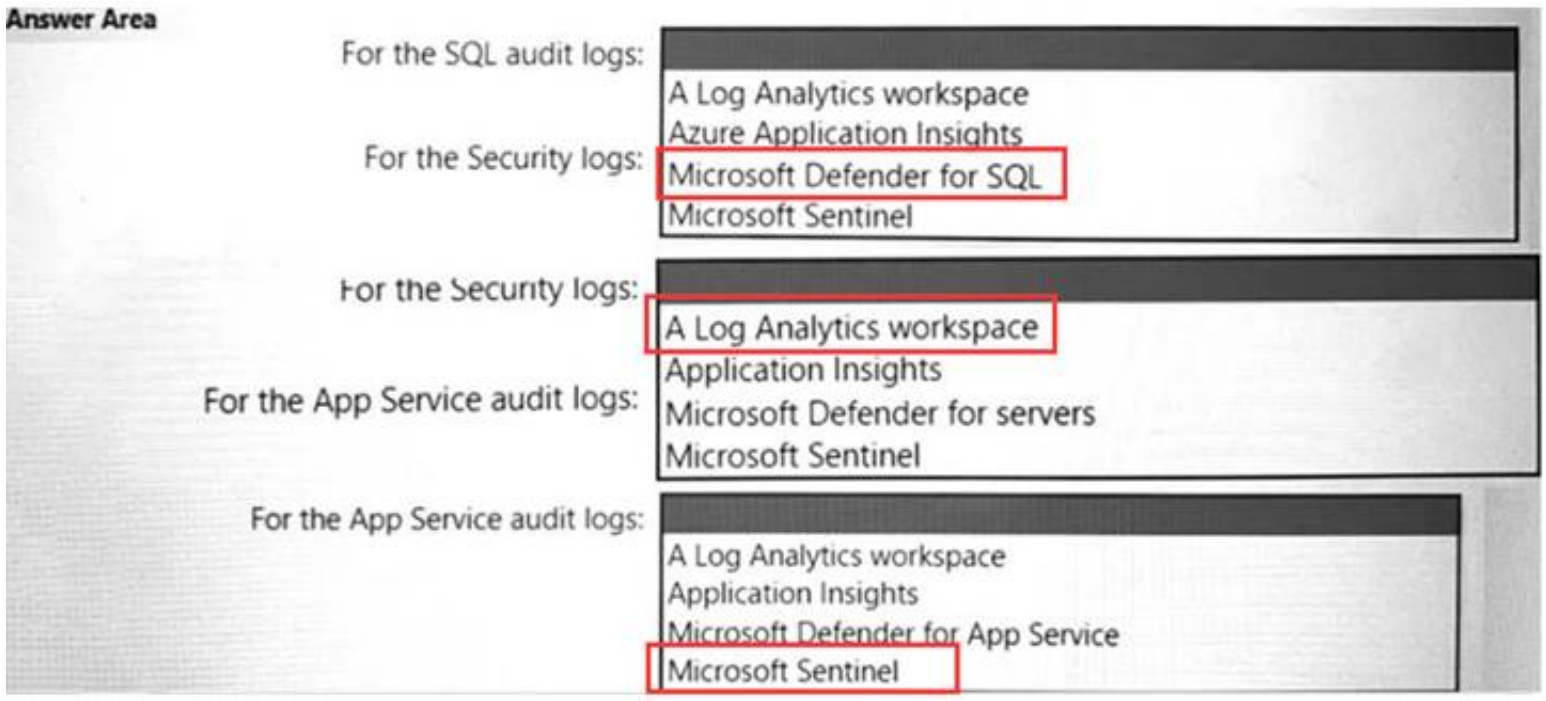
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 143
- (Exam Topic 3)
You have 50 Azure subscriptions.
You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.
B. Assign a policy to each subscription.
C. Assign a policy to a management group.
D. Assign an initiative to each subscription.
E. Assign a blueprint to each subscription.
F. Assign a blueprint to a management group.

Answer: AF

Explanation:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

NEW QUESTION 147
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend

NEW QUESTION 148
.....

Relate Links

100% Pass Your SC-100 Exam with Exambible Prep Materials

https://www.exambible.com/SC-100-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/